

**Remarks/Arguments:**

By this amendment, Applicant has amended claims 1, 21-23, 25, 27 and 28. Claims 1-28 are pending.

**Information Disclosure Statement**

The Examiner has not considered the Supplemental Information Disclosure Statement filed February 3, 2004 claiming that it "fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance . . . of each patent listed that is not in the English language." Applicant respectfully disagrees. The Supplemental Information Disclosure Statement in question lists one U.S. Patent, and five foreign patent documents. Only one of the foreign patent documents is not in English. But as to the foreign patent document not in English, Applicants have included a European Search Report which identifies the relevance of this document. It is Applicant's contention that this is a sufficient basis for the Examiner to review this one foreign patent document, as well as all of the other documents cited in the Supplemental Information Disclosure Statement. Applicant's position is supported by the MPEP at Section 609(III)A(3). Applicant therefore requests that the Examiner review, consider and acknowledge all of the documents cited in the Supplemental Information Disclosure Statement filed February 3, 2004.

**Claim Rejections Under Section 102**

Claims 1-28 stand rejected under 35 U.S.C. §102(e) as being anticipated by Chaum. By this Amendment, Applicant respectfully traverses this Section 102(e) rejection. In addition, Applicant questions whether the Examiner intended to reject claims 1-28 under subsection (e) of Section 102. Applicant would appreciate clarification on this issue.

Claims 1, 12, 14, 17, 21, 22, 23, 25, 27 and 28 are independent claims. Claims 2-11 are dependent on claim 1. Claim 13 is dependent on claim 12; claims 15 and 16 are dependent on claim 14; claims 18-20 are dependent on claim 17; and claim 26 is dependent on claim 25.

Applicant will discuss the basis for Applicant's traversal of each of the independent claims in turn.

**Claim 1**

Claim 1 is directed to an equipment authentication and cryptographic communication system and includes the following feature:

- said system-end equipment receives said individual user-end equipment information from said user-end equipment, reproduces said individual user-end equipment secret information from said received individual user-end equipment information.

This feature is neither taught nor suggested in the Chaum Patent.

The Chaum Patent in general relates to an automatic real time highway toll collection system with one or more roadside collection stations communicating over a short-range by high speed bidirectional microwave communication links with one or more in-vehicle units associated with one or more respectively corresponding vehicles in one or more traffic lanes of a highway. At least two up-link communication sessions and at least one down-link communication session are transacted in real time during the limited duration of a roadside collection station communication footprint, as a vehicle travels along its lane past a highway toll plaza.

More particularly, the Chaum Patent discloses at column 7, lines 66 to column 8, line 4 that "(t)he Reload Computer may be installed with an internal Kryptor (a high speed RSA/DES encryption device) mounted in an ISA expansion slot. The Kryptor (a high speed RSA/DES encryption device) **generates blank electronic checks and balance data** tier transmission to a remote Reload Station" (emphasis added). It is apparent from this statement that the Chaum Patent does not disclose a system reproducing the individual user-end equipment secret information from the received individual user-end equipment information as set forth in Applicant's claimed invention.

In addition, claim 1 includes the following additional feature:

- said user-end equipment and said system-end equipment execute a cryptographic communication with each other using said individual user-end equipment secret information.

The Office Action takes the position that this feature is taught at column 9, lines 36-48 with respect to Figures 2A and 2B of the Chaum Patent. Applicants respectfully disagree. While the discussion in the identified portion of the Chaum Patent relative to Figures 2A and 2B discuss the operation of a downlink timing controller so as to prevent interference between adjacent lanes in a multi-lane environment, Applicant does not find any teaching or suggestion in the above-identified portion of the Chaum Patent (or any other portion of the Chaum Patent) of the requirement that the user-end equipment and the system-end equipment execute a cryptographic communication with each other using individual user-end equipment secret information.

Based on the foregoing remarks, Applicant respectfully submits that claim 1 and dependent claims 2-11 are patentably distinguished from the Chaum Patent.

#### **Claim 12**

Claim 12 is directed to an equipment authentication and cryptographic communication system and includes among its features the following:

- said system-end equipment is provided with a second system converter for **generating said user-end equipment secret information by a system conversion of the user-end equipment information received from said user-end equipment, a second encryption unit and second decryption unit.**

This feature is somewhat similar to the feature of claim 1 noted-above for reproducing the individual user-end equipment secret information, but is more detailed in its requirements. The Office Action takes the position that this feature is taught in the Chaum Patent at column 9, lines 25-48. Applicant respectfully disagrees. The identified portion of the Chaum Patent as discussed above, concerns Figures 2A and 2B and the operation of a downlink timing controller for preventing interference between adjacent lanes in a multi-lane environment. But as noted above, this portion of the Chaum Patent simply does not teach or suggest the above noted feature of claim 12 concerning the generation of the user-end equipment secret information.

Based on the foregoing, Applicant respectfully submits that independent claim 12 and dependent claim 13 are patentably distinguished from the Chaum Patent.

**Claim 14**

Claim 14 concerns a method of equipment authentication and cryptographic communication for an equipment authentication and cryptographic communication system. Claim 14 includes among its steps the following:

- receiving said user-end equipment information from said user-end equipment, and **generating said user-end equipment secret information from said user-end equipment information received in said user-end equipment.**

This step is similar to the requirement noted above with respect to claim 1 and for the same reasons as noted above, Applicant respectfully submits that claim 14, as well as claims 15 and 16, are patentably distinguished from the Chaum Patent.

**Claim 17**

Claim 17 is directed to a cryptographic communication system including among its features, the following:

- said authentication equipment includes **a means for producing said secret key particular to said IC card from said certificate of individual IC card key data received, a first decryption unit for reporting said response data by decrypting said encrypted data received from said IC card** using said produced secret key.

This feature is also similar to the feature noted above with respect to claim 1, and on the basis of the remarks stated above with respect to claim 1, Applicant respectfully submits that claim 17 and dependent claims 18-20 are patentably distinguished from the Chaum Patent.

**Claims 21-23, 25, 27, and 28**

Applicant has amended claims 21-23, 25, 27, and 28 to more clearly define the authentication requirement of these claims and the matching determination requirement of these claims. It is Applicant's contention that these amendments are not the addition of new matter but are based on the application as originally filed.

Claims 21, 23, and 27 relate to an electronic toll collection authentication system, and claims 22, 25 and 28 relate to an electronic toll collection authentication method. The authentication systems and methods defined by these claims are disclosed with respect to Figures 2, 3 and 4 of the subject application.

The Office Action has taken the position that each of these claims is anticipated by the Chaum Patent. Applicant respectfully disagrees. In rejecting each of these claims, the Office Action cites portions of the Chaum Patent which discuss, in very general terms, the operation and structure of the automatic real-time highway toll collection system of Chaum. But it is Applicant's contention that the specifically defined electronic toll collection authentication system and method set forth in independent claims 21-23, 25, 27 and 28 are simply not taught or suggested in the Chaum Patent. Applicant below identifies those portions of each of these claims which are not taught or suggested in the Chaum Patent. On the basis of the lack of disclosure of these features, Applicant contends that these claims, and the claims dependent thereon, are patentably distinguished from the Chaum Patent.

Claim 21 is directed to an electronic toll collection authentication system and includes the following features which are not taught or suggested in the Chaum Patent:

- said card including . . . a response data transmission means for transmitting IC card ID data and a certificate of individual IC card key data, together with said encrypted data stored in said encrypted data storage means, as response data to said roadside equipment.
- said roadside equipment including a dividing means for dividing said transmitted response data; a second decryption means for decrypting said certificate of

individual IC card key data divided by said dividing means, using a validation key; a first matching determination means for making a matching determination of said IC card ID produced as a result of decryption with another IC card ID provided by said dividing means; a first decryption means for producing response data for decrypting an encrypted data provided by said dividing means; and a challenge data transmission means for transmitting said challenge data to said IC card; and

- said ETC authentication system providing authentication of said IC card ID by said roadside equipment by authenticating said certificate of individual IC card key data received with said IC card ID, and said central processing equipment providing a matching determination of said response data encrypted by said IC card and decrypted by said roadside equipment to said challenge data.

Claim 22 is directed to an electronic toll collection authentication method and includes steps which are similar to the features noted above in claim 21. At least based on any one of the features noted above with respect to claim 21, claim 22 is likewise patentably distinguished from the Chaum Patent.

Claim 23 is directed to an electronic toll collection authentication system and includes the following features which are not taught nor suggested in the Chaum Patent:

- said IC card including . . . a response data transmission means for transmitting an IC card ID data and a certificate of individual IC card key data, together with said encrypted data as a response data to a second roadside equipment,
- said second roadside equipment including a first dividing means for dividing said response data; a second encryption means for decrypting said certificate of individual IC card key data divided by said first dividing means, using a validation key; a first matching determination means for providing a matching determination if an IC card ID produced as a result of decryption with another IC card ID provided by said first dividing means; and a first decryption means for producing a response data by decrypting an encrypted data obtained from said first dividing means,

- central processing equipment including a second dividing means for dividing said challenge data and said IC card ID generated by said first roadside equipment; a third dividing means for dividing said response data and said IC card ID decrypted by said second roadside equipment;
- a second matching determination means for making a matching determination of said challenge data obtained by said second dividing means and said response data provided by said third dividing means, and
- said ETC authentication system providing authentication of said IC card ID by said second roadside equipment by authenticating said certificate of individual IC card key data received with said IC card ID.

Claim 25 is directed to an electronic toll collection authentication method and includes steps which are similar to the above noted features of claim 23. It is Applicant's contention that at least based on any one of the above noted features similar to those of claim 23, claim 25 is patentably distinguished from the Chaum Patent.

Claim 27 concerns an electronic toll collection authentication system that includes among its features the following features which are not taught nor suggested in the Chaum Patent:

- said IC card including . . . a response data transmission means for transmitting an IC card ID data and a certificate of individual IC card key data, together with said encrypted data as response data to second roadside equipment;
- said second roadside equipment including a first dividing means for dividing said response data; a decryption means for decrypting said certificate of individual IC card key data divided by said first dividing means, using a validation key; a first matching determination means for providing a matching determination of said IC card ID produced as a result of decryption with another IC card ID provided by said first dividing means; and a first decryption means for decrypting an encrypted data provided by said first dividing means to obtain response data,

- central processing equipment including a second dividing means for dividing said challenged data and IC card ID generated in said first roadside equipment; a third dividing means for dividing said response data decrypted in said second roadside equipment and said IC card ID; and a second matching determination means for providing a matching determination of said challenge data obtained in said second dividing means and said response data obtained in said third dividing means; and
- said ETC authentication system providing authentication of said IC card ID by said second roadside equipment by authenticating said certificate of individual IC card key data received with said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC card and decrypted by said second roadside equipment.

Claim 28 is directed to an electronic toll collection authentication method and includes similar features noted above with respect to claim 27. It is Applicant's position that claim 28 is patentably distinguished from the Chaum Patent at least based on any one of the above noted features of claim 27.

Claims 21-23, 25, 27, and 28 are more specific in their defining of the electronic toll collection authentication system and method of Applicant's claimed invention. And these more specific features and steps are simply not found in the Chaum Patent; particularly the sections of the patent identified in the Office Action which are very broad and general in their description of the Chaum highway toll collection system.

Based on the foregoing remarks, Applicant respectfully submits that independent claims 20-23, 25, 27 and 28, as well as the claims dependent thereon, are patentably distinguished from the Chaum Patent because the above noted features of these claims are not taught or suggested in the Chaum Patent.

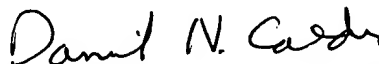


Appln. No.: 09/432,007  
Amendment Dated: June 25, 2004  
Reply to Office Action of: March 11, 2004

MAT-VO7838

In view of the foregoing remarks and amendments, Applicant respectfully submits that claims 1-28 are in condition for allowance. Reconsideration and allowance of all pending claims are respectfully requested.

Respectfully submitted,



---

Daniel N. Calder, Reg. No. 27,424  
Attorney for Applicant

DNC/dlm/ds

Dated: June 25, 2004

P.O. Box 980  
Valley Forge, PA 19482  
(610) 407-0700

The Commissioner for Patents is hereby authorized to charge payment to Deposit Account No. 18-0350 of any fees associated with this communication.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

June 25, 2004



---

DLM\_I:\MAT\VO7838\AMEND01.DOC